HASIL CEK_60020397_Point-C13-IRD-850GB-Forensic Analysis WhatsApp Mobile Application On Android-Based Smartphones Using National Institute of Standard and Technology (NIST) Framework

by Imam Riadi 60020397

Submission date: 11-Dec-2020 09:44AM (UTC+0700)
Submission ID: 1471636456
File name: ational_Institute_of_Standard_and_Technology_NIST_Framework.pdf (986.82K)
Word count: 4378
Character count: 24327

International Journal of Cyber-Security and Digital Forensics (IJCSDF) 8(3): 223-231
The Society of Digital Information and Wireless Communications (SDIWC), 2019 ISSN: 2305-0011

Forensic Analysis WhatsApp Mobile Application On Android-Based Smartphones Using National Institute of Standard and Technology (NIST) Framework

Vindy Arista Yuliani[1], Imam Riadi[2]
[1]*Department of Informatics, Universitas Ahmad Dahlan, Yogyakarta, Indonesia*
[2]*Department of Information System, Universitas Ahmad Dahlan, Yogyakarta, Indonesia*
(vindy1300018124@webmail.uad.ac.id, imam.riadi@is.uad.ac.id)

ABSTRACT

The Whatsapp application is an alternative to exchange messages because of its ease of use. The number of WhatsApp users and security features is available, allowing WhatsApp to be used as a communication medium for criminal purposes such as fraud of buying and selling online, terrorist activities, planning murder, and other criminal activities. Message archives stored on WhatsApp applications installed on cellular phones can be used by investigators as evidence to uncover crimes that use this application as their communication media. The mobile forensic method uses the National Institute of Standard and Technology (NIST) with preservation, acquisition, examination and analysis, reporting. This study describes on the application of mobile forensics which can be used as a reference for conducting forensic research on whatsapp applications to obtain evidence in the form of conversation messages by extracting whatsapp application databases that store encrypted conversation messages. Exploration results using oxygen forensic and andriller assistance will be used as research reports with the involvement of android smartphone evidence.

Keywords: Android, WhatsApp, NIST, Forensics, Mobile.

1. INTRODUCTION

Data security is very important in maintaining the confidentiality of information, especially sensitive information, which only authorized parties may know. Information which is the result of processing data has different values for each person [1]. Where the authenticity of information is very important at the time of delivery or when the information is received [2].

The Android operating system is one of the operating systems operated on smartphones [3]. Since its development in 2005 and was first released in 2008 [4]. Android is an open source operating system, because of the open source nature that many developers have developed several applications that can run on an Android system.

WhatsApp application is a new alternative in exchanging messages because of the ease of use. Users can send messages freely to anyone who also uses the WhatsApp application [5]. Can be seen in Figure 1 and Figure 2.

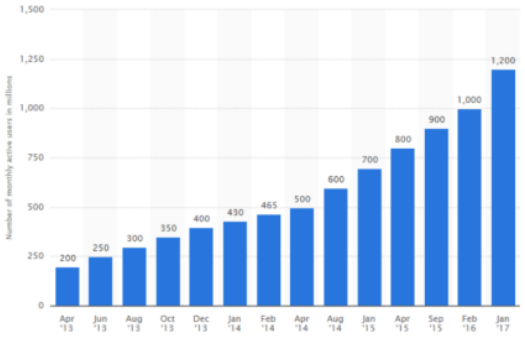

Figure 1. The statistics of whatsapp user

Figure 2. The statistics of whatsapp messages

In Figure 1 and Figure 2 will explain the number of users of the WhatsApp application. In January 2017, there are active WhatsApp users of 1.2 billion per month. The number has increased compared to the number of WhatsApp users in February 2016, which as many as 1 billion active users each month and can be seen graphically every month shows that whatsapp users always experience an increase. WhatsApp application every day to deliver message delivery as much as 42 billion.

WhatsApp provides many features such as message sending, group chat, video calls, file sending, telephone, and is equipped with encryption for data security. The number of WhatsApp users and security features is available, allowing WhatsApp to be used as

a communication medium for criminal purposes such as drug trafficking, terrorist activities, murder planning, and other criminal activities [6].

This study describes the application of mobile forensics which can be used as a reference for conducting forensic investigations on whatsapp applications and obtaining evidence in the form of conversation messages by extracting whatsapp application database that stores encrypted conversations and then conducts forensic investigation reports with the involvement of smartphone evidence.

2. LITERATURE REVIEW

References [7] conducted a forensic analysis on WhatsApp with taking evidence at Android smartphone devices and extracting data on smartphone devices using the python programming.

References [8] illustrates research on the Decryption of Encrypted WhatsApp Databases on Non-Rooted Android Devices is used in retrieving evidence on smartphone devices with several comparisons of data extraction tools performed to take an approach that not only allows message recovery, but also can help retrieve deleted messages.

References [9] conducting forensic analysis on WhatsApp that successfully extracts chat conversations stored in internal and external memory using the WhatsApp key extractor and decryptor to convert the backup database into a text database that can be seen in the SQLite database browser.

References [10] illustrates research on conduct comparative evaluation forensic tools that serve to extract artifacts in the form of messages, images, videos and documents with NIST forensic methodology in the latest version of WhatsApp in Android-based devices. The tools used are ADB, WhatsApp Key/DB Extractor 4.7, and Belkasoft Evidence (trial version). Forensic tools are tested to run the WhatsApp database extraction and decryption process that has been updated with .crypt12 end-to-end encryption. The results of extraction, decryption, and validation of forensic tools will be compared to have the conclusions.

References [11] illustrates research on evaluate the comparison results analys tools on blackberry messenger using oxygen forensic, andriller, and autopsy. The results of the comparison analysis of this forensic tool will be presented at the reporting stage. The stages of comparative analysis conducted using NIST Mobile Forensics Framework.

3. BASIC THEORY

3.1 Forensics

Forensic meaning of the word is "presenting to the court" while the term "forensics" is derived from the Latin word relating to the law or apply scientific analysis in the context of the law. Digital Forensics is a scientific process or a scientific effort that is based on the science of collecting, analyzing and presenting evidence in a court proceeding to assist the disclosure of a crime through disclosure of evidence authorized by the laws and regulations [12].

3.2 WhatsApp Messenger

WhatsApp adalah aplikasi pesan untuk smartphone yang mampu berjalan lintas platform diantaranya ; Apple iOS, BlackBerry, Android, Symbian Nokia Series 40 dan Windows Phone. WhatsApp Messenger menggunakan paket data internet sama halnya seperti layananan email, browsing web, dan layanan instant messengers lainnya. Aplikasi WhatsApp Messenger menggunakan koneksi data mobile serta WiFi untuk melangsungkan komunikasi data, dengan menggunakan WhatsApp, seseorang dapat melakukan obrolan online, berbagi file, bertukar foto dan fitur lainnya yang menarik penggunanya [13].

3.3 Oxygen Forensic

Oxygen Forensic Suite is a forensic software for extraction and analysis of data from cell phones, smartphones and tablets. This tool offers several hash algorithms and one of which can be selected in each investigation case. Oxygen Forensic Suite also has the capability to provide general information about the smartphone and the network that the device was connected to. The other useful capability from this tool is recovered all contacts, SMS, MMS, and user's files [14].

3.4 Andriller

Andriller is a utility which consists of various tools for serving various purposes which includes cracking of screen lock pattern, PIN and passwords, decoding of encrypted databases and files, data extraction automatically and unpacking of android backups. This tool kit solves many of mobile forensics needs for the Android OS [14].

4. RESEARCH METHOD

The stages of this research were conducted to determine the extent of abuse committed in the WhatsApp application. The method used in this study is guided by the mobile forensic method of the National Institute of Standard and Technology (NIST) which has several stages that writer describes can be seen in Figure 3.

Figure 3. Stage of Whatsapp Messenger research.

4.1 Preservation

It is the initial stage which includes the process of collecting, searching, and documenting evidence. In this process, evidence is maintained so no data changes occur.

4.2 Acquisition

At acquisition is the stage that performs the imaging process or cloning a mobile device.

4.3 Examination and Analysis

The examination and analysis phase aims to reveal and analyze the results of the acquisition stage to obtain evidence.

4.4 Reporting

The process of compiling a summary in detail, namely, reporting the results of the analysis includes a description of actions that explain the selected tools and procedures, to determine other actions that need to be done and provide recommendations to improve policies, procedures, equipment, and other aspects of the forensic process [15].

5 RESULTS AND DISCUSSION

5.1 Preservation

Preservation is the initial stage in mobile forensic methods. some steps that the investigator needs to do, first the investigator is obliged to conduct a search, collection and documentation of evidence data. The sample used for testing this research as evidence analysis is in the form of two smartphones that have been screened as evidence in a crime case. Both smartphones are rooted with the condition of the active screen security feature. At this stage documentation is carried out with both smartphones. Can be seen at Table 1 is the result of evidentiary specification documentation.

Table 1. Specifications of Evidence

Perpetrator's Smartphone

Alias	EVERCOSS A28A
Retail Name	EVERCOSS A28A
Internal Name	Android Phone
Platform	Android OS
IMEI	357673050823619
Software Revision	4.4.4
Rooted	Yes
IMSI	510103962885213
S/N	SANZDWKB6RG7TTGSOV8
Extracted by version	6.4.0.67
Extraction started	11/11/2018 21:16:49
Extraction finished	11/11/2018 21:47:27

Victim Smartphone

Alias	SM-G530H
Retail Name	SM-G530H
Internal Name	Android Phone
Platform	Android OS
IMEI	356396062072915
Software Revision	5.0.2
Rooted	Yes
IMSI	356396062072915
S/N	f64deee2
Extracted by version	6.4.0.67
Extraction started	03/10/2018 23:34:32
Extraction finished	04/10/2018 07:07:45

5.2 Acquisition

The stage of acquisition is the stage of investigators who perform imaging on the internal memory and external memory of the offender smartphone and the victim's smartphone. On each Android smartphone device the method of retrieving data may vary depending on the type of vendor and several other things such as the transfer protocol, security conditions on the screen that is active or not, and the version of the android. Types on mobile devices and evidence data that will be carried out by extractors generally determine tools and techniques that can be used in case of investigation [9].

There are various ways to retrieve data on an Android smartphone. In this study the investigator used the help of Oxygen forensics, Whatsapp Viewer, and Andiller. Each tool has its own advantages and disadvantages, it is caused by the influence of the condition of the smartphone such as root access rights, USB debugging, screen security, vendor type, android version, and supporting transfer protocols.

Smartphone Detection

Smartphone detection is done with oxygen forensics and Andriller to acquire original data obtained. In the second detection the smartphone is connected to the PC to do an investigation on Oxygen forensics and Andriller with active screen security features, so that the smartphone can enable USB debugging and both smartphones can perform the

imaging process with the detection of smartphones on Oxygen forensics and Andriller. Table 2 shows the initial process of detecting smartphones with Oxygen forensics.

Table 2. Smartphone Acquisition by using Oxygen Forensik

Evidence	Condition	Transfer Protocol	External Memory	Internal Memory
Perpetrator's Smartphone	Rooted	MTP	Detected	Detected
Victim Smartphone	Rooted	MTP	Detected	Detected

On the smartphone the perpetrator and the victim's smartphone will wait for the physical dump process, the length of time needed depends on how much memory is available on each smartphone. Where the extracted memory is internal memory and external memory, and how much data is stored in that memory.

The data that must be extracted on the perpetrator's smartphone is 5.46Gb. While the data that must be extracted on the smartphone is a victim of 14.73Gb. Can be seen in Figure 4 and Figure 5.

Figure 4. physical dumb perpetrator's smartphone

Figure 5. physical dump victim's smartphone

Settling the data extraction stage on both smartphones to look for evidence that will be used by the investigator at the stage of examination & analysis.

While the data search process carried out using Andriller generates HTML and integrated reports that contain all extraction data from the perpetrator's smartphone and victim's smartphone. Can be seen in Figure 6 and Figure 7.

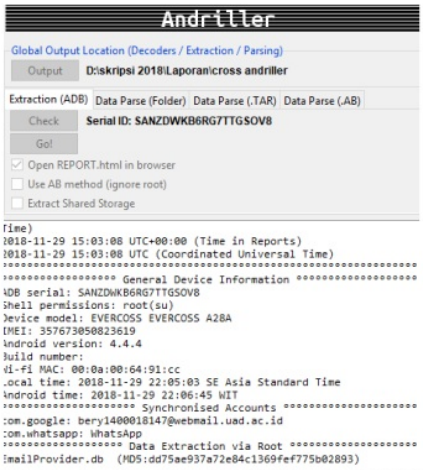

Figure 6. extraction process of perpetrator's smartphone

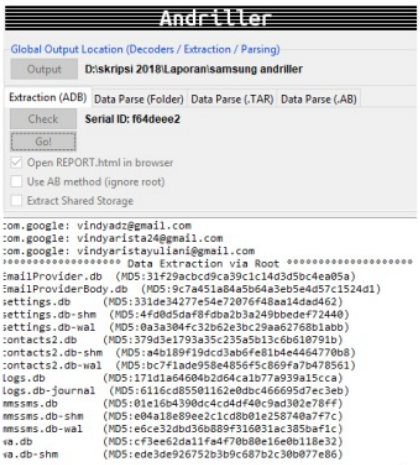

Figure 7. extraction process of victim's smartphone

5.3 Examination And Analysis

The stage of examination and analysis aims to analyze the data on the results of the acquisition to obtain data relating to whatsapp applications from the perpetrator's smartphone and victim's smartphone. At this stage, use some help tools to analyze the results of the imaging data that has been done before by using Oxygen forensics, WhatsApp Viewer, and Andriller.

Whatsapp Database Extraction

1. Extraction of Whatsapp Database with Oxygen forensics

In database extraction the results of the explorer whatsapp folder and com.whatsapp folder are done with Oxygen forensics to get the database results on the perpetrator's smartphone, while the victim smartphone will retrieve the database and whatsapp key. Can be seen at Table 3.

Tabel 3. Folder a results Extraction and WhatsApp Data Explorer

Evidence	Storage	Folder Explorer Data
Perpetrator's Smartphone	Internal Memory External Memory	Folder *com.whatsapp*
Victim Smartphone	Internal Memory	Folder *com.whatsapp*

In the data folder explored it looks the same in the com.whatsapp folder storage. Can be seen in Figure 8.

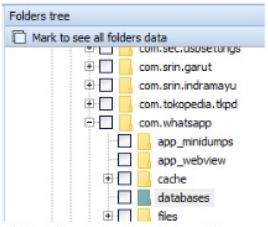

Figure 8. Folder Storage explorer data com.whatsapp

In the data storage folder Explore com.whatsapp there are .db files and whatsapp keys that will be needed by the investigator. Can be seen in Figure 9.

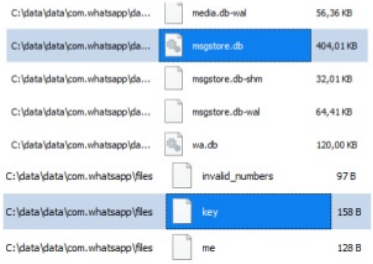

Figure 9. file .db and key whatsapp at folder com.whatsapp

2. Extraction of Whatsapp Database with Andriller

The result of extracting the database using Andriller explores the wa.db folder. All data that has been extracted in Andriller can be seen in the browser window in the form of a plaint text report and a link to view the contents of the extracted report Can be seen in Figure 10 and Figure 11.

[Andriller Report] SAMSUNG SM-G530H | I

Type	Data
ADB serial:	f54deee2
Android ID:	a0d76b8ea316cfa2
Shell permissions:	root(su)
Manufacturer:	SAMSUNG
Model:	SM-G530H
IMEI:	Unknown
Android version:	5.0.2
Build name:	
Wifi MAC:	00:f4:6f:01:aa:43
Bluetooth MAC:	00:f4:6f:01:aa:42
Bluetooth name:	vindy arista
Local time:	2018-11-29 16:27:02 SE Asia Standard Time
Android time:	2018-11-29 16:27:01 WIB
Accounts:	com.google.android.gms.matchstick: Duo com.whatsapp: WhatsApp com.google: ahmadi .@gmail.com com.google: pin J@gmail.com com.google: rusul. "@gmail.com com.google: sulis "@gmail.com com.google: vinc @gmail.com com.google: vindyL i@gmail.com com.google: vindya i@gmail.com
Security (Gesture Hash):	da39a3ee5e6b4b0d3255bfef95601890afd80709
Security (Lockscreen Pattern):	None
Security (Lockscreen Hash):	88ACA1844DA49ACC10747B4B0636A2431251EE
Security (Lockscreen Salt):	1144351751038644435
System:	Synchronised Accounts (9)
System:	Wi-Fi Passwords (506)
System:	Android Download History (10)
Web browser:	Google Chrome History (28)
Communications data:	Contacts (771)
Communications data:	Samsung Call logs (495)
Communications data:	Samsung SMS Snippets (500)
Communications data:	SMS Messages (433)
Applications data:	WhatsApp Contacts (501)
Applications data:	WhatsApp Calls (702)
Applications data:	WhatsApp Messages (13,499)

Figure 10. Report.html in browser victim's Smartphone

[Andriller Report] EVERCOSS EVERCOSS A28A | IMEI:357673050823619

Type	Data
ADB serial:	SANZDWKB6RG7TTGSOV8
Android ID:	4a4d5efe17cf7472
Shell permissions:	root(su)
Manufacturer:	EVERCOSS
Model:	EVERCOSS A28A
IMEI:	357673050823619
Android version:	4.4.4
Build name:	
Wifi MAC:	00:0a:00:64:91:cc
Local time:	2018-11-29 22:05:03 SE Asia Standard Time
Android time:	2018-11-29 22:06:45 WIT
Accounts:	com.google: bery14000 @webmail.uad.ac.id com.whatsapp: WhatsApp
System:	Synchronised Accounts (2)
System:	Wi-Fi Passwords (10)
Web browser:	Android Web Browser Passwords (1)
Web browser:	Android Web Browser History (172)
System:	Android Download History (59)
Communications data:	Contacts (125)
Communications data:	Call logs (51)
Communications data:	SMS Messages (25)
Applications data:	WhatsApp Contacts (41)
Applications data:	WhatsApp Calls (1)
Applications data:	WhatsApp Messages (144)

Figure 11. Report.html in browser perpetrator's Smartphone

Decrpt the WhatsApp Database

1. Decrypt the WhatsApp Database with Oxygen forensics

At the decrypt stage, whatsapp database all data that can be decrypted by the investigator. because whatsapp database that has been obtained is still crypt12 encrypted. In order to open the cyprt12 investigator uses oxygen forensics to open an encrypted WhatsApp database on the offender's smartphone and use the help of WhatsApp Viewer to open an encrypted WhatsApp database on the victim's smartphone. Can be seen in Figure 12.

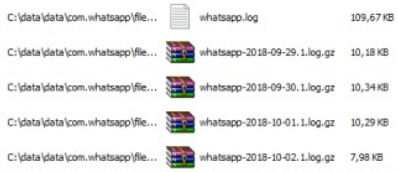

Figure 12. database in perpetrator's smartphone

Conversation data on the perpetrator's smartphone can be viewed directly on categories/massages/Privatechat. In the private chat there is the contents of the conversation that is used as evidence. Where data on smartphone actors do not need to use whatsapp viewer help to view conversation message sessions Can be seen in Figure 13.

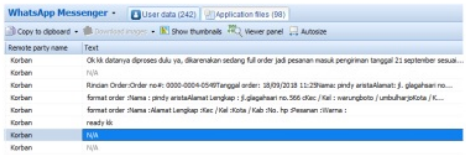

Figure 13. conversation in perpetrator's smartphone

Investigator will then decrypt the WhatsApp database which is still crypt12 encrypted on the victim's smartphone. The victim's smartphone database cannot be opened only by using Oxygen Forensics, so the process of describing the victim's smartphone database is done using the help of whatsapp viewer to open the conversation message. Retrieving the database on the victim's smartphone uses the help of ES File Explorer tools to get crypt12 and whatsapp keys. Can be seen in Figure 14.

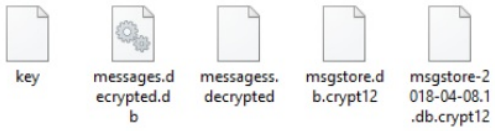

Figure 14. Database crypt12 at victim's smartphone

Massages.decrypted whatsapp is an encrypted database file. Where the results of decrypting crypt12 are done using whatsapp viewer by selecting the file menu and then selecting crypt12, then selecting file.db and whatsapp key in the storage folder. Can be seen in Figure 15.

Figure 15. messages.decrypted whatsapp

The conversation message on the victim's smartphone database that has been encrypted can be opened by opening messages.decrypted whatsapp via whatsapp viewer. Can be seen in Figure 16.

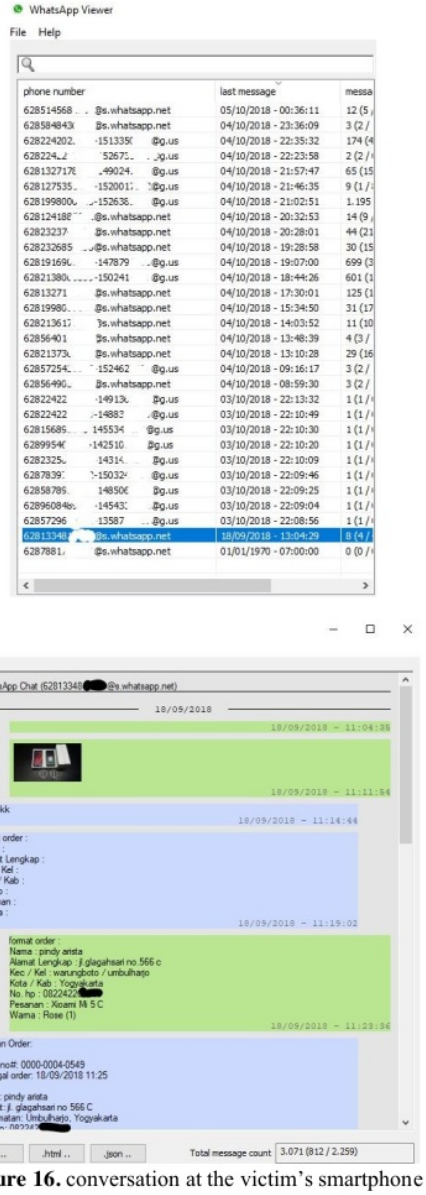

Figure 16. conversation at the victim's smartphone

2. Decrypt the WhatsApp Database with Andriller

The process of decrypting the WhatsApp database using andriller assistance will be applied to the offending smartphone and victim smartphone. database that is still encrypted can be decrypted without having to open the whatsapp folder and com.whatsapp folder. Where the wa.db file is directly extracted to md5 and from the extraction results md5 is decrypted into plain text. Can be seen in Figure 17.

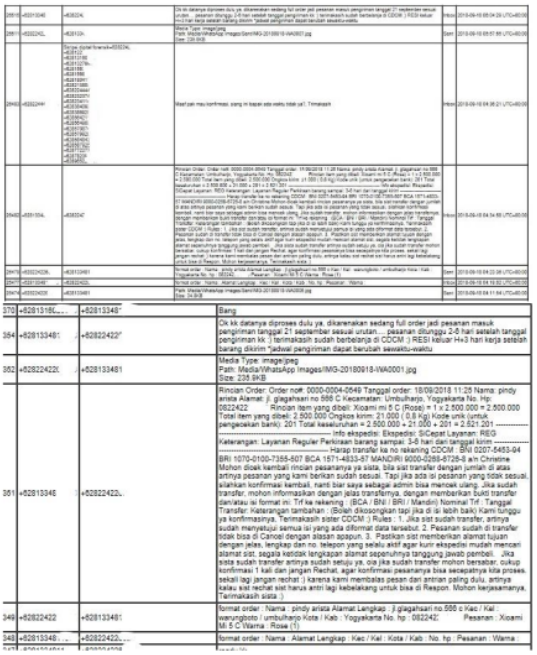

Figure 17. Encrypt md5 result in plain text form

5.4 Reporting

After analyzing the smartphone of the perpetrator and the smartphone victim, the process of applying mobile forensics to digital artifacts on Android smartphones related to the WhatsApp application does not only get conversations and profile photos. Media files that have been sent or received are audio, video, voice note, images, and call history files. All files can be in one conversation message, but in this study only create conversation message scenarios that contain text and images only. Table 4 below is important information about the comparison of extraction and exploratory results on whatsapp done with oxygen forensics and andriller.

Table 4. Extraction and Exploration Data Results Folder on Whatsapp with Oxygen forensics and Andriller.

Information	Oxygen Forensic		Andriller	
	Perpetrator's Smartphone	Victim Smartphone	Perpetrator's Smartphone	Victim Smartphone
Smartphone Type	EverCross A28A	Samsung SM-G530H	EverCross A28A	Samsung SM-G530H
User Mobile Number	081334 81xxxx	082242 26xxxx	-	-
Application Version	2.18.248	2.18.248	2.18.248	2.18.248
User Name	Pelaku	Korban	0813348 1xxxx	082242 26xxxx
Whatsapp Contact	43	568	41	501
Conversation	8	8	7	6
Encrypted Databases	12	12	12	12
Avatar	1	1	-	-
Profile Pictures	1	1	-	-
WhatsApp audio	-	-	-	-
WhatsApp calls	-	-	-	-
WhatsApp images	-		2	2
WhatsApp profile photo	-	-	-	-
WhatsApp video	-	-	-	-

The extraction results from the perpetrator's smartphone and victim's smartphone that have been explored in the WhatsApp app conversation message using Oxygen Forensic help get EverCross A28A and Samsung SM-G530H smartphone types, 08133481xxxx User telephone numbers and 08224226xxxx, Application Versions obtained on both smartphones the same is 2.18.248, Username Perpetrator's and Victim Username, WhatsApp contact on the offender smartphone 43 and whatsapp contact victim 568, conversations obtained on both smartphones are the same 8, database encryption obtained on both smartphones is the same as cyprt12, avatar found on both smartphones with 1, profile photos obtained on both smartphones with 1, and oxygen forensics did not get images in whatsapp conversions because whatsapp data could not be loaded. While the extraction results from the perpetrator's smartphone and the victim's smartphone that has been explored in whatsapp application conversation messages using Andriller's help get the EverCross A28A and Samsung SM-G530H smartphone types, the Application Version obtained

on both smartphones is 2.18.248, User Name obtained on both smartphones use the telephone number used 08133481xxxx and 08224226xxxx, Whatsapp contacts on the perpetrator 41 smartphone and whatsapp contact victim 501, conversations obtained on both smartphones are not the same 7 and 6, database encryption obtained on both smartphones is the same as cyprt12, andriller cannot display avatars and photo profile, and andriller get whatsapp images on both smartphones with the same number, namely 2. Differences in results from oxygen forensic tools and andriller tools are also seen in the image in the conversation message. In figure 18, you can see the image obtained using oxygen forensic tools, namely N / A, which means there is a message received but the message is empty. While in figure 19 shows the results of the images obtained using andriller tools, which are text messages that show the existence of image messages, image storage folders on whatsapp, and the size of images sent / received.

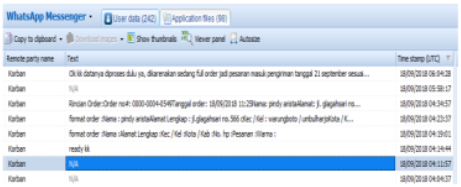

Figure 18. Image result from tools oxygen forensik

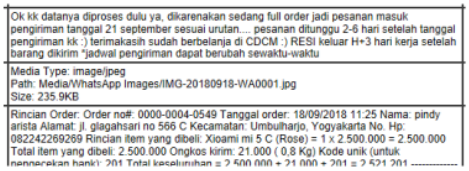

Figure 19. Image result from tools andriller

In the \data\data\com.whatsapp\databases\ directory There are several unencrypted databases and in the \data\data\com.whatsapp\avatar\files\ directory there are thumbnails of user profile photos and contacts on the whatsapp application. To view avatars and other media files such as photos, videos and more can be opened at oxygen forensics.

To see cell phone contacts can be seen through the whtasapp application file that has been extracted with oxygen forensics in the categories contacts. In the categories contacts there are not only whatsapp user contacts, there are also contacts stored on the smartphone. In addition, there is also information about the identity of users of the WhatsApp application that is read in the categories contacts.

The categories of contacts are located in the wa.db file storage which can be opened in the oxygen forensic application. Can be seen in Figure 20.

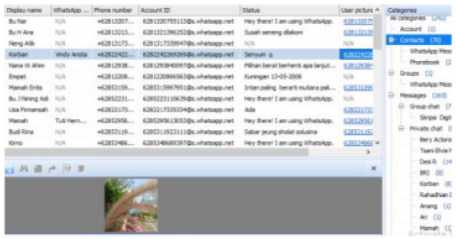

Figure 20. Categories contacts

The WhatsApp application automatically backs up conversations every day at 2:00 am in a SQLite3 database and when there are changes to the addition or removal of WhatsApp application conversations. The conversation will be backed up automatically at 2:00 a.m. with a different date. Whatsapp application data is in two folders, the first folder is the com.whatsapp folder contained in the \ data \ data \ com.whatsapp directory in the Android system partition, while the second folder is the whatsapp folder which is in internal memory and SD Card with cyprt12 extension.

To access the WhatsApp folder, which is located on the internal memory or SD card, you don't need to need root privileges, even ordinary users can open the WhatsApp folder. In the WhatsApp folder there is a media file that has been sent or received on the WhatsApp application and there is an encrypted conversation database. the database cannot be opened without using root privileges and whatsapp keys to open the wa.db file to decrypt the message. Can be seen in Figure 21.

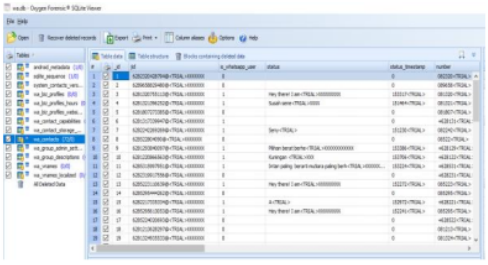

Figure 21. File wa.db at SQLite3 database

Techniques in decrypting the database application WhatsApp has different ways, depending on the type of smartphone and the type of encryption used. In whatsapp viewer to use crypt8 encryption type and crypt12 must use Key to decrypt the database. The crypt8 and crypt12 encrypted database cannot be decrypted using the Key on a different smartphone, where each smartphone installed by the WhatsApp application will create a unique Key that can only be used by the smartphone itself. Some Android smartphones cannot do imaging on system partitions and internal memory, this is one of the obstacles in conducting mobile forensics on the Android platform. And there are several other things that make mobile

forensic processes more difficult to do, namely if the smartphone's SD card has been encrypted, so the process will become more complicated, besides if the internal or external memory has been repeatedly formatted, it is only less likely to get data the desired data is returned, due to limited memory space which results in the old data being accumulated with new.

6 CONCLUSION

The mobile Forensic application whatsapp application on an Android-based smartphone is used to get digital evidence on the whtasapp application installed on the offender's smartphone and the victim's smartphone. On both smartphones different artifacts were carried out by using oxygen forensic and andriller help to open the crypt12 database, which showed conversational data suspected of being a crime or fraud committed. With the application of mobile forensic analysis, this study succeeded in obtaining artifact evidence in the form of exploration of smartphone data reports such as chat sessions, avatars, contacts on whatsapp applications, status on whatsapp, and also getting whatsapp media files and encrypted backup database files.

7 REFERENCES

[1] H. Abdurachman and E. Gunadhi, "Security of SMS Data Communication on Android using the Advanced Encryption Standard (AES) Cryptographic Application," *J. Algoritm. Sekol. Tinggi Teknol. Garut*, vol. 12, no. 1, pp. 1–6, 2015.

[2] N. B. Nugroho, Z. Azmi, and S. N. Arif, "Email Security Application Using RC4 Algorithm," *J. Ilm. saintikom (sains dan Komput.*, vol. 15, no. 3, pp. 81–88, 2016.

[3] H. Supriyono, A. . Saputra, E. Sudarmilah, and R. Darsono, "Designing hadith learning applications for android-based mobile devices," vol. 8, no. 2, pp. 907–920, 2014.

[4] I. Defni, Rahmayun, "Jurnal Momentum ISSN : 1693-752X SMS (Short Message Service) Encryption on Android-based Cellular Phones with RC6 Method Jurnal Momentum ISSN : 1693-752X," vol. 16, no. 1, pp. 63–73, 2014.

[5] A. R. Pratama, "Whatsapp Forensics: Exploration of File Systems and Databases on Android And Ios Applications," *J. Teknoin*, vol. 20, no. 1, pp. 1–11, 2016.

[6] G. M. Zamroni, R. Umar, and I. Riadi, "Forensic Analysis of Android Instant Messaging Applications," in *Prosiding ANNUAL RESEARCH SEMINAR*, 2016, vol. 2, no. 1, pp. 102–105.

[7] S. Sahu, "An analysis of whatsapp forensics in android smartphones," *J. Eng. Res.*, vol. 3, no. 5, pp. 349–350, 2014.

[8] G. Lp and J. Ky, "Information Technology & Software Engineering WhatsApp Forensics : Decryption of Encrypted WhatsApp Databases on Non Rooted Android Devices," vol. 5, no. 2, pp. 2–5, 2015.

[9] Y. N. Kunang and A. Khristian, "Implementation of forensic procedures for whatsapp applications on android phones," *Annu. Res. Semin.*, vol. 2, no. 1, pp. 59–68, 2016.

[10] R. Umar, I. Riadi, and G. M. Zamroni, "Mobile Forensic Tools Evaluation for Digital Crime Investigation," *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 8, no. 3, p. 949, 2018.

[11] I. Riadi, R. Umar, and A. Firdonsyah, "Forensic tools performance analysis on android-based blackberry messenger using NIST measurements," *Int. J. Electr. Comput. Eng.*, vol. 8, no. 5, pp. 3991–4003, 2018.

[12] A. Kurniawan, I. Riadi, and A. Luthfi, "Forensic analysis and prevent of cross site scripting in single victim attack using open web application security project (OWASP) framework," *J. Theor. Appl. Inf. Technol.*, vol. 95, no. 6, pp. 1363–1371, 2017.

[13] N. Anwar and I. Riadi, "Analisis Investigasi Forensik WhatsApp Messanger Smartphone Terhadap WhatsApp Berbasis Web," *J. Ilm. Tek. Elektro Komput. dan Inform.*, vol. 3, no. 1, p. 1, 2017.

[14] I. Riadi, Sunardi;, and A. Firdonsyah, "Forensic Investigation Technique on Androids Blackberry Messenger using NIST Framework," *Int. J. Cyber-Security Digit. Forensics*, vol. 16, no. 4, pp. 198–205, 2017.

[15] I. Riadi, A. Yudhana, M. Caesar, and F. Putra, "Forensic Tool Comparison on Instagram Digital Evidence Based on Android with The NIST Method Forensic Tool Comparison on Instagram Digital Evidence Based on Android with The NIST Method," no. November, 2018.

HASIL CEK_60020397_Point-C13-IRD-850GB-Forensic Analysis WhatsApp Mobile Application On Android-Based Smartphones Using National Institute of Standard and Technology (NIST) Framework

ORIGINALITY REPORT

8%	8%	2%	2%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	insightsociety.org Internet Source	2%
2	core.ac.uk Internet Source	2%
3	www.jatit.org Internet Source	2%
4	www.ijcaonline.org Internet Source	1%
5	Heri Nurdiyanto, Robbi Rahim, Nur Wulan. "Symmetric Stream Cipher using Triple Transposition Key Method and Base64 Algorithm for Security Improvement", Journal of Physics: Conference Series, 2017 Publication	1%

Exclude quotes	On	Exclude matches	< 1%
Exclude bibliography	On		